Michigan Cybersecurity SAAABA Briefing

Presenter:
Laura Clark, Acting Chief Security Officer for the State, DTMB

DTMB | Cybersecurity & Infrastructure Protection

State of Cybersecurity: Attacks and Data Breaches

- Identity theft impacts **60 million** Americans
- U.S. spent over ***$15 billion*** on cybersecurity in 2019
- Cost of the average data breach to a U.S. company: $7.91 million
- Federal Government phishing encounter rates rose from 17% in the fourth quarter 2019 to 40% in the first quarter of 2020
  - The increase has been tied to COVID-19 but there ha been an upward trend in mobile phishing since the beginning of 2019
- Mobile phishing attacks rose 37 percent in the first quarter of 2020 from the last quarter of 2019

Source: Symantec 2019 Internet Security Threat Report

Source: Reuters


“If we’re careful, we’ll be protected, right?”

It CAN (and Will) Happen to Anyone

novator &

a

at focuses
nputing,
ficial

ebsite)

hacked on

er one in

"At least 34 percent of U.S. consumers
experienced a data compromise within 2018..."

From a WFSA-12 broadcast,
"State warns about hackers stealing data from personal phones."

https://www.wsfa.com/2019/07/12/state-warns-about-hackers-stealing-data-personal-phones/

"We took a hacker to a café and, in **20 minutes**, he knew where everyone else was born, what schools they attended, and the last five things they googled."

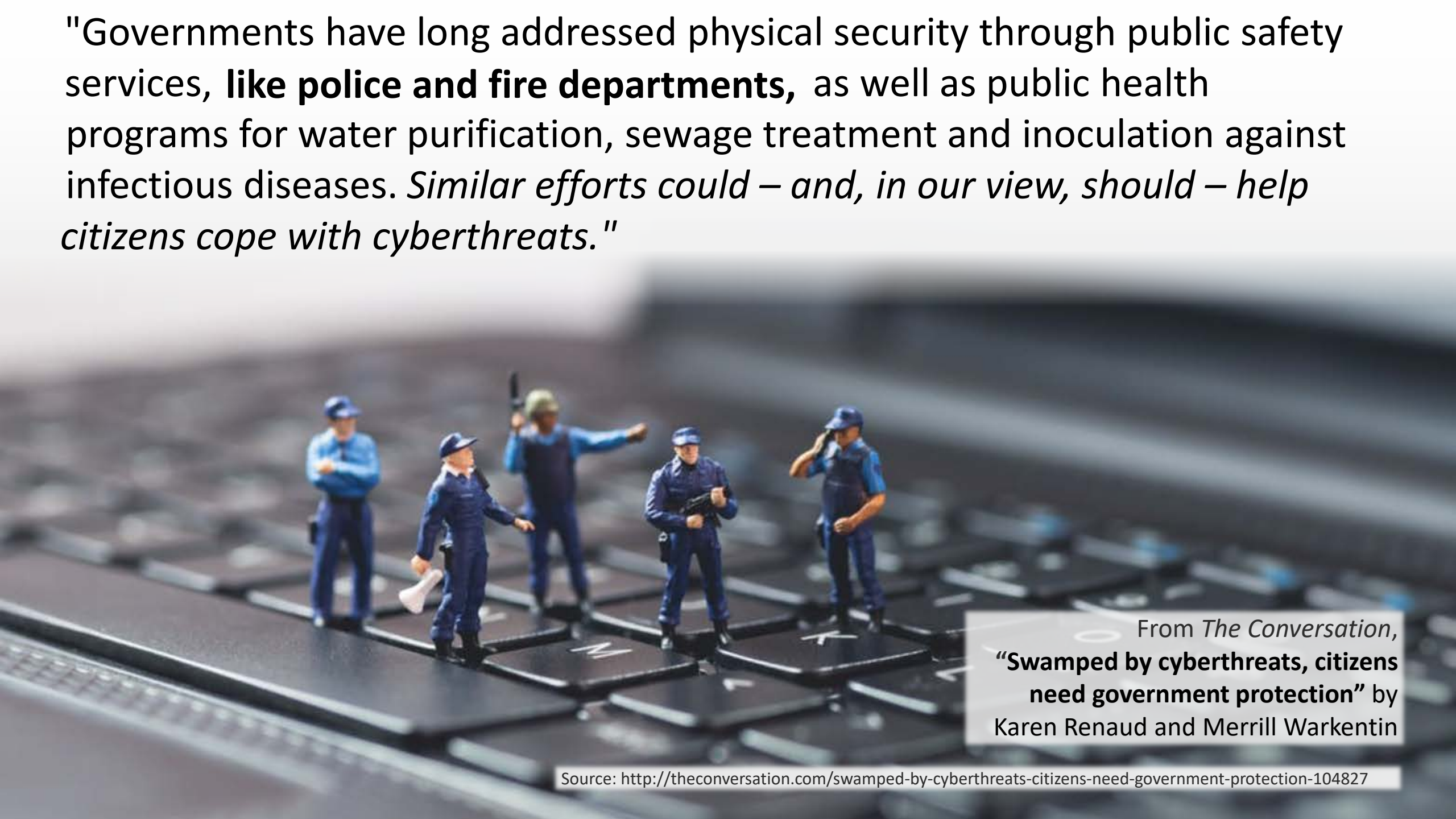
From a Medium.com article titled,
"Maybe Better If You Don't Read This Story on Public WiFi"
by Maurits Martijn

Source: https://medium.com/matter/heres-why-public-wifi-is-a-public-health-hazard-dd5b8dcb55e6

“Mobile devices have
LARGE VULNERABILITIES
and without mobile threat defense,
you can't see them
and therefore, *you can't defend against them.*”

-John Michelsen, Zimperium CTO

"Governments have long addressed physical security through public safety services, **like police and fire departments,** as well as public health programs for water purification, sewage treatment and inoculation against infectious diseases. *Similar efforts could – and, in our view, should – help citizens cope with cyberthreats."*



From *The Conversation*, **"Swamped by cyberthreats, citizens need government protection"** by Karen Renaud and Merrill Warkentin

Source: http://theconversation.com/swamped-by-cyberthreats-citizens-need-government-protection-104827

State Government is a Target

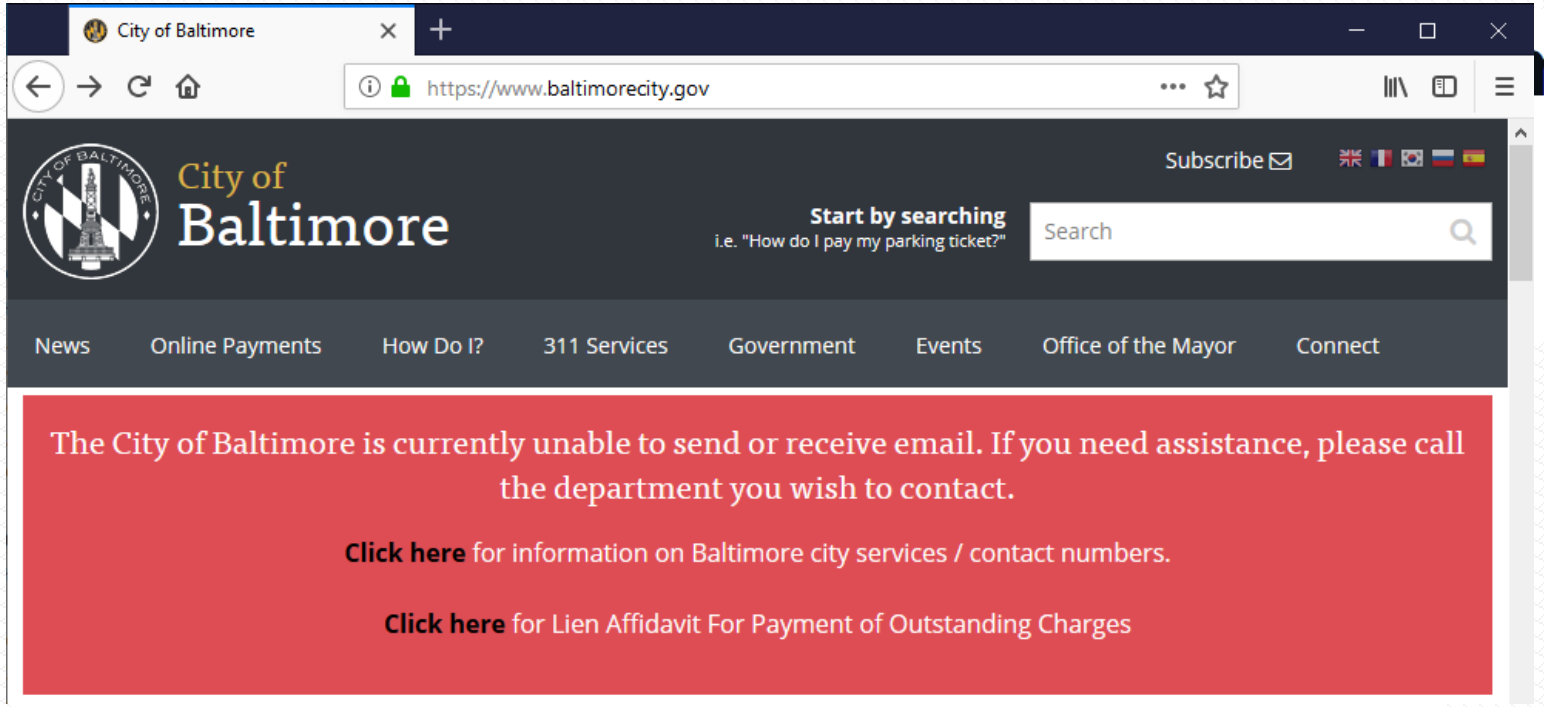
46,774 views | Aug 19, 2019, 04:09am

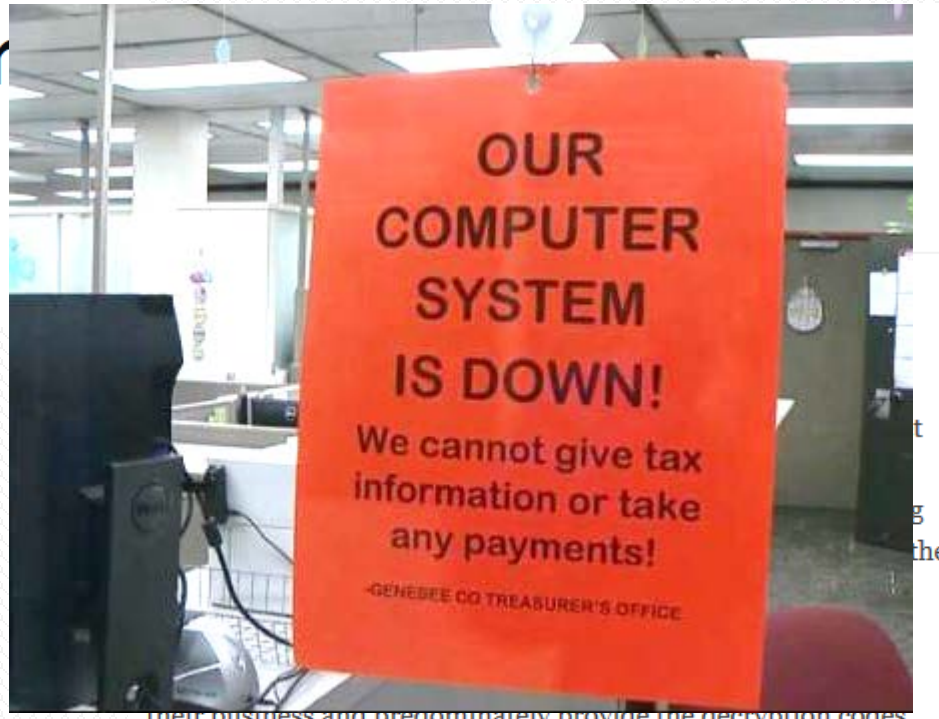
After an Initial Ransomware Attack, Colorado DOT Gets Hit Again

The original attack in late February has morphed and re-infected a portion of the transportation agency's remaining computers, according to officials.

BY TAMARA CHUANG, THE DENVER POST / MARCH 2, 2018

Cyber Attacks Are Not Statistics





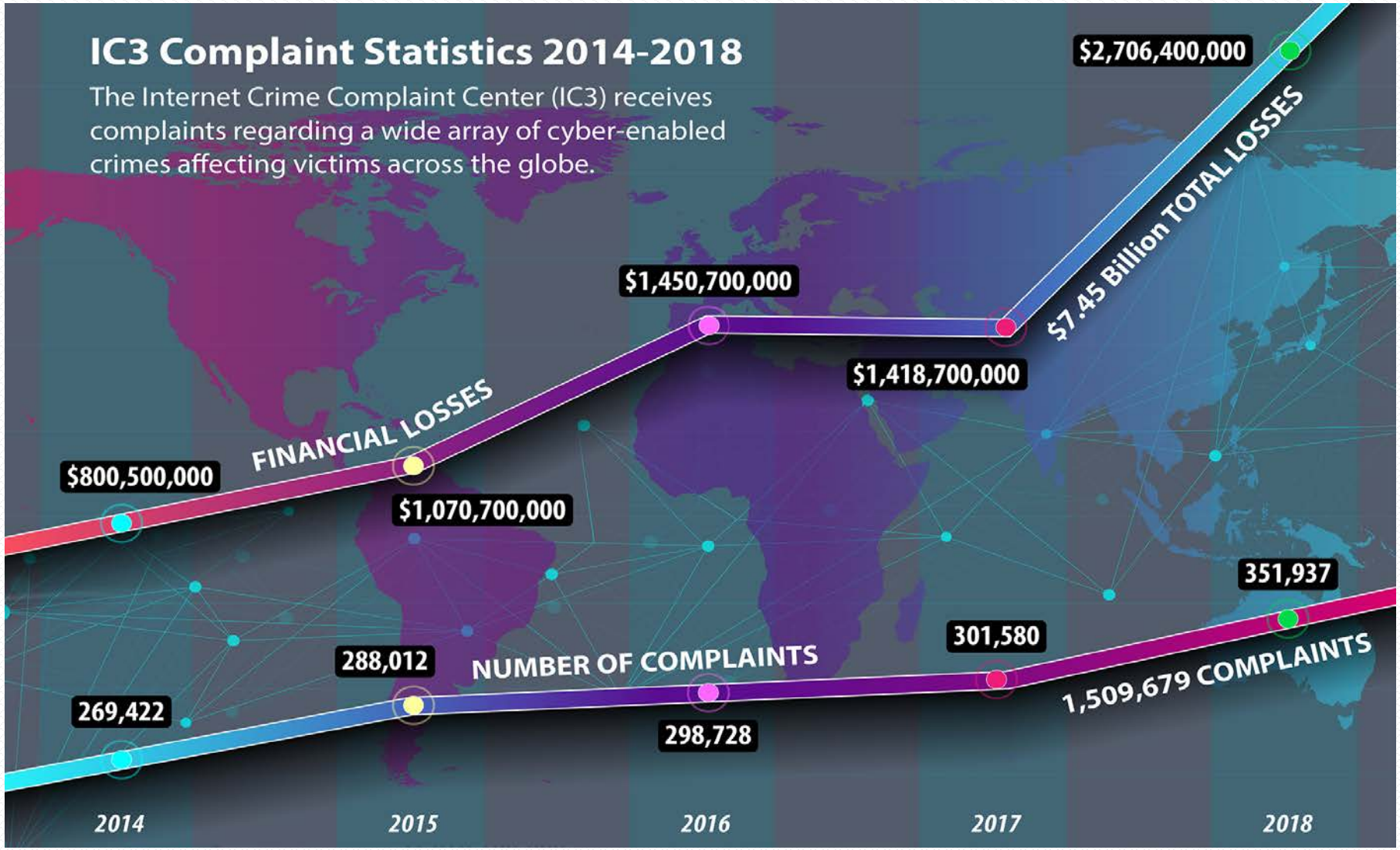
By Ionut Ilascu July 14, 2019 02:05 PM

Another public administration in the U.S. surrenders cybercriminal demands as La Porte County, Indiana, pays $130,000 to recover data on computer systems impacted by ransomware.

their business and predominately provide the decryption codes once the ransom is paid."

They have a genuine impact on businesses and people's lives.

Financial Losses On The Rise

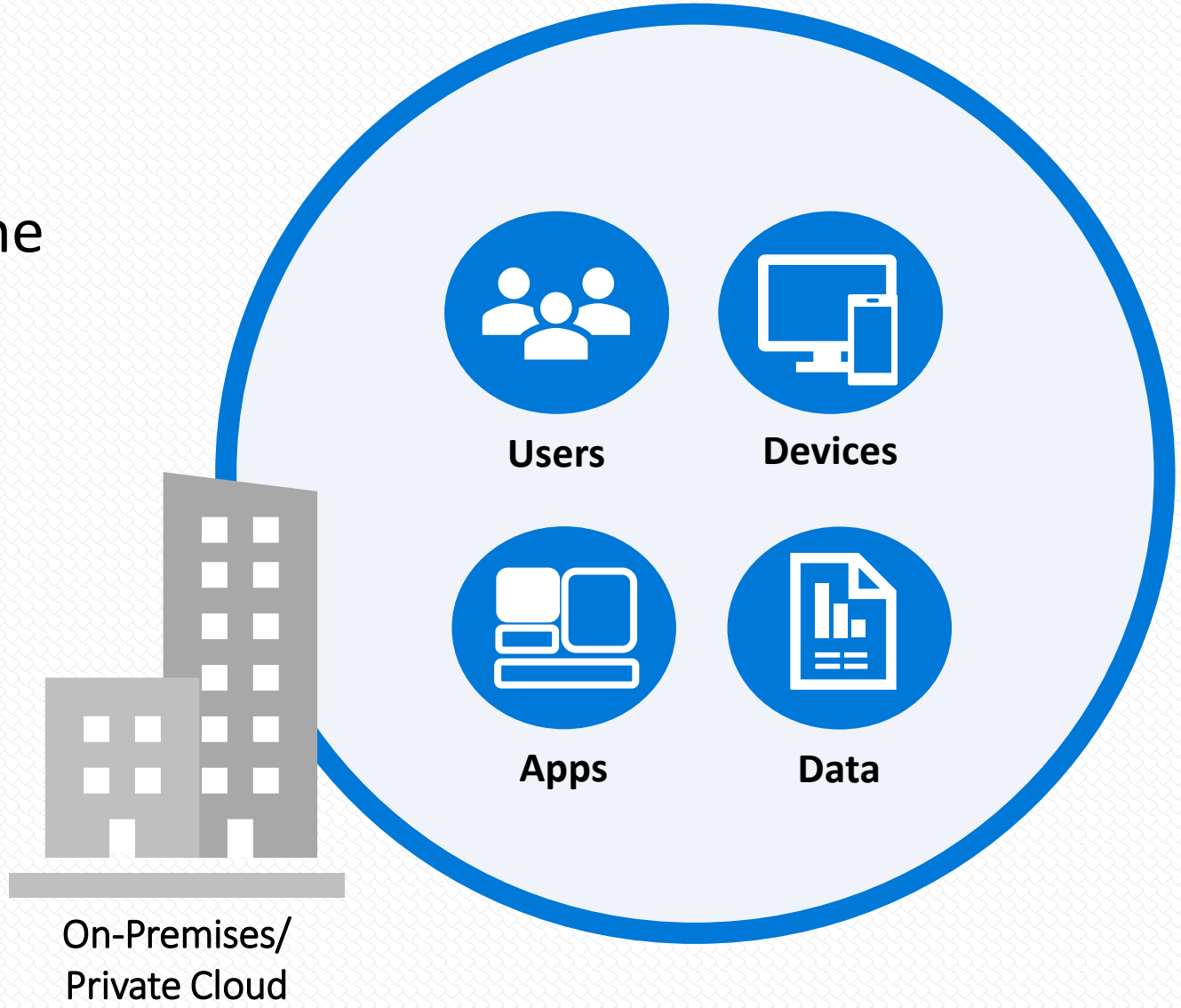


- Survey Question

Cybersecurity Ecosystem Overview

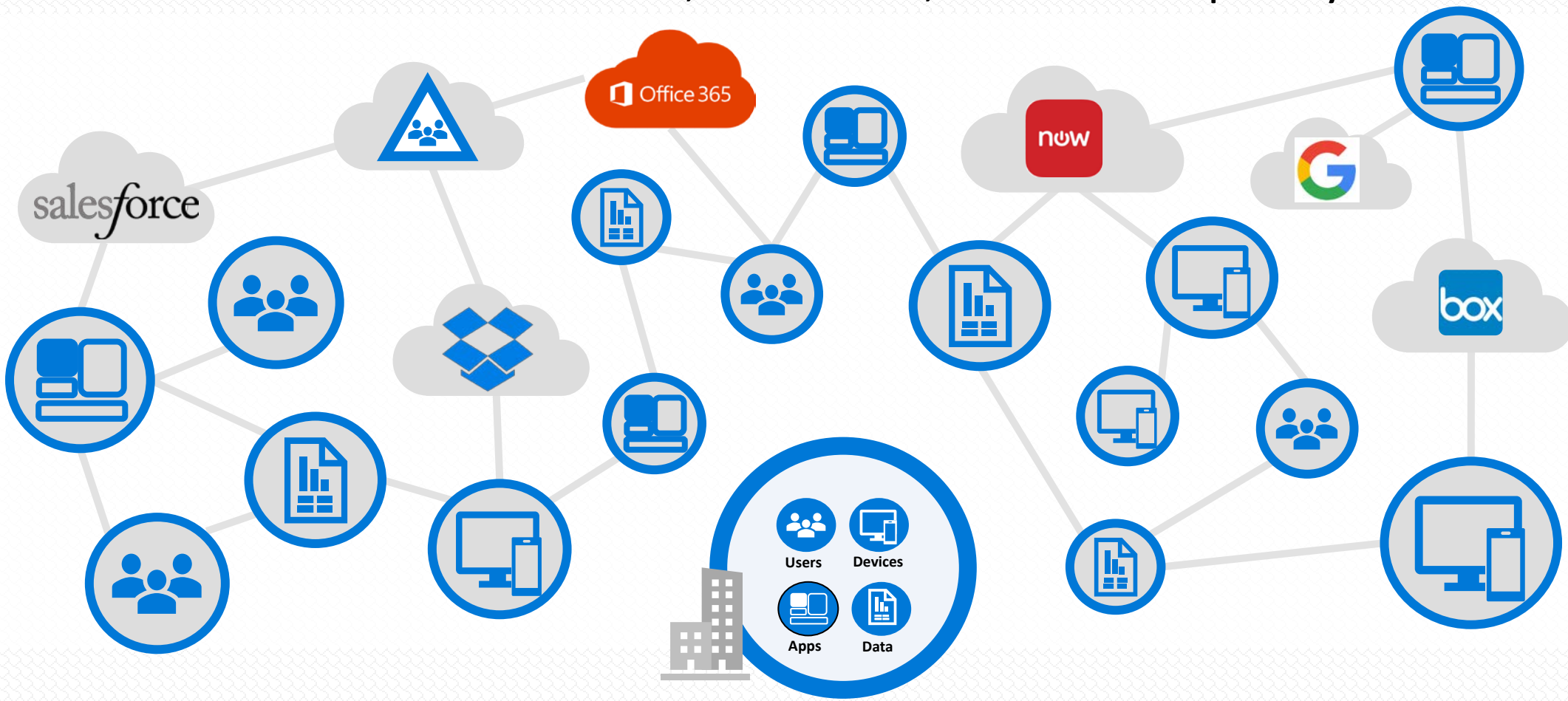
Legacy Security

In the past, the firewall was the **security perimeter**.

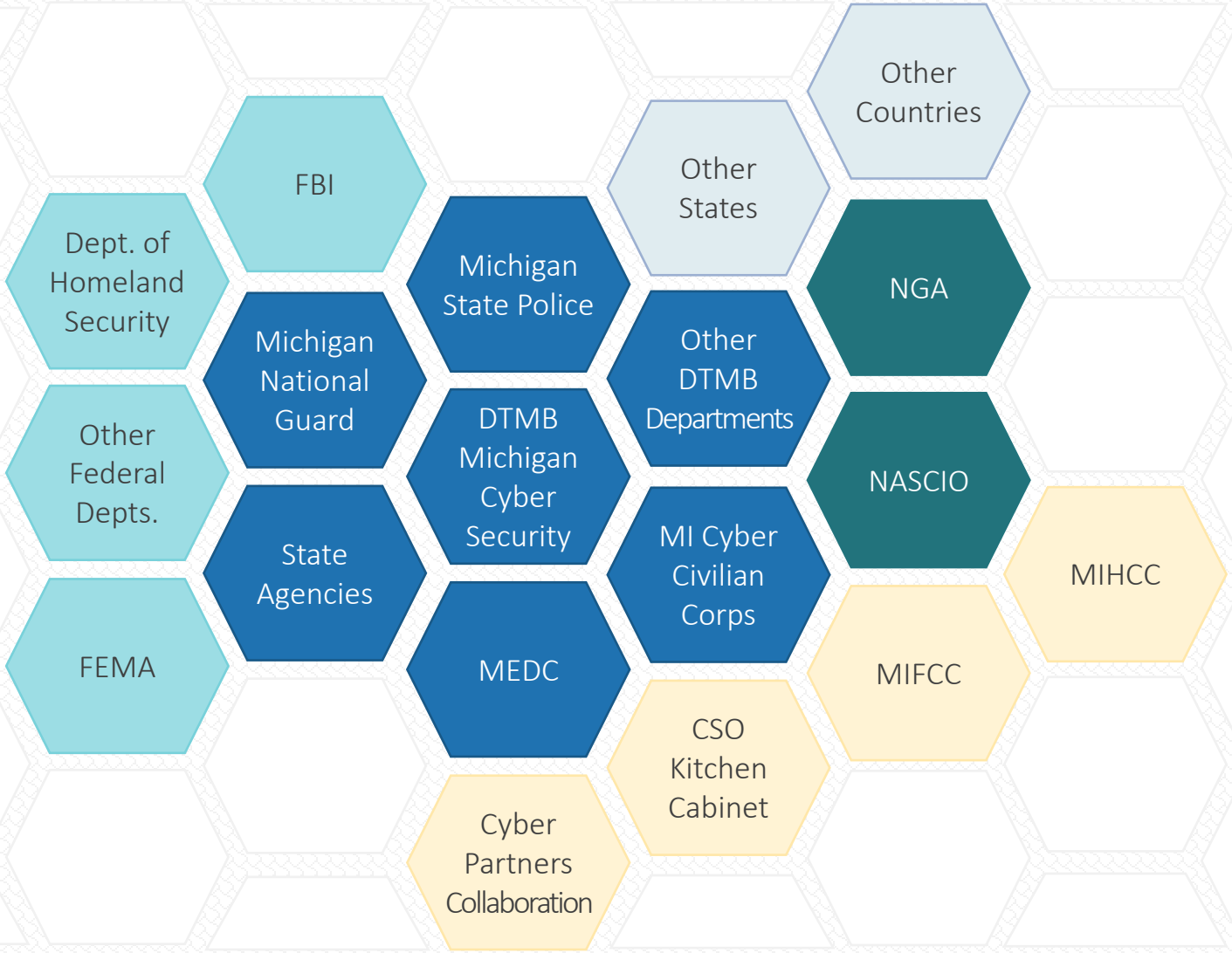


The New Digital Reality

Now there are **blended boundaries**, more data, & more complexity.



Cybersecurity Ecosystem



Michigan Stepping Up to Cybersecurity

2011

- First annual Michigan Cyber Summit.
- Cyber Initiative created.

2012

- Michigan Cyber Range launched.
- NGA Cyber Resource Center for States.
- Cyber Support at DNC.
- CSO Kitchen Cabinet formed.

2013

- The Michigan Cyber Command Center opened.
- *Michigan Cyber Disruption Response Strategy* published.
- NASCIO Cybersecurity Award.
- Michigan Financial and Healthcare Cybersecurity Councils formed.

2014

- Michigan Cyber Civilian Corps launched.
- Michigan and Israel signed bilateral cooperation agreement on cybersecurity.
- Various cyber hubs opened around SOM.

Michigan Stepping Up to Cybersecurity

2015

- *Michigan Cyber Disruption Response Plan* published.
- State Emergency Operations Center (SEOC) opened.
- Statewide Risk Mgmt. program launched.
- MING Army CPT.

2016

- Regional Cybersecurity Education Collaboration piloted.
- High School Cyber Challenge formed.
- MING Air CPT.

2017

- CSO50 awarded the Cyber Disruption Response Plan to SOM.
- MiC3 was awarded the State Scoop IT Innovation of the Year Award.

2018

- DTMB successfully finishes the CISOaaS pilot.
- PA 132 “Cyber Civilian Act” passed, providing a framework for MiC3.
- DTMB embarked on SOC 2.0 project.
- DTMB established a Security Accreditation Process (MiSAP) for IT Assets.

Michigan Stepping Up to Cybersecurity

2019

- Launched Cyber Partners Collaboration Forum.
- Cyber Functional Exercise held with activation of State Emergency Operations Center (SEOC) opened.

2020

- Homeland Security Grant Funding to provide cyber training to local government.
- Expanding the Marshall Plan to secure public schools.
- Initial Innovative Readiness Training (IRT) event.
- Revising the CDRP.
- Enhance the Security Awareness Program.

2021

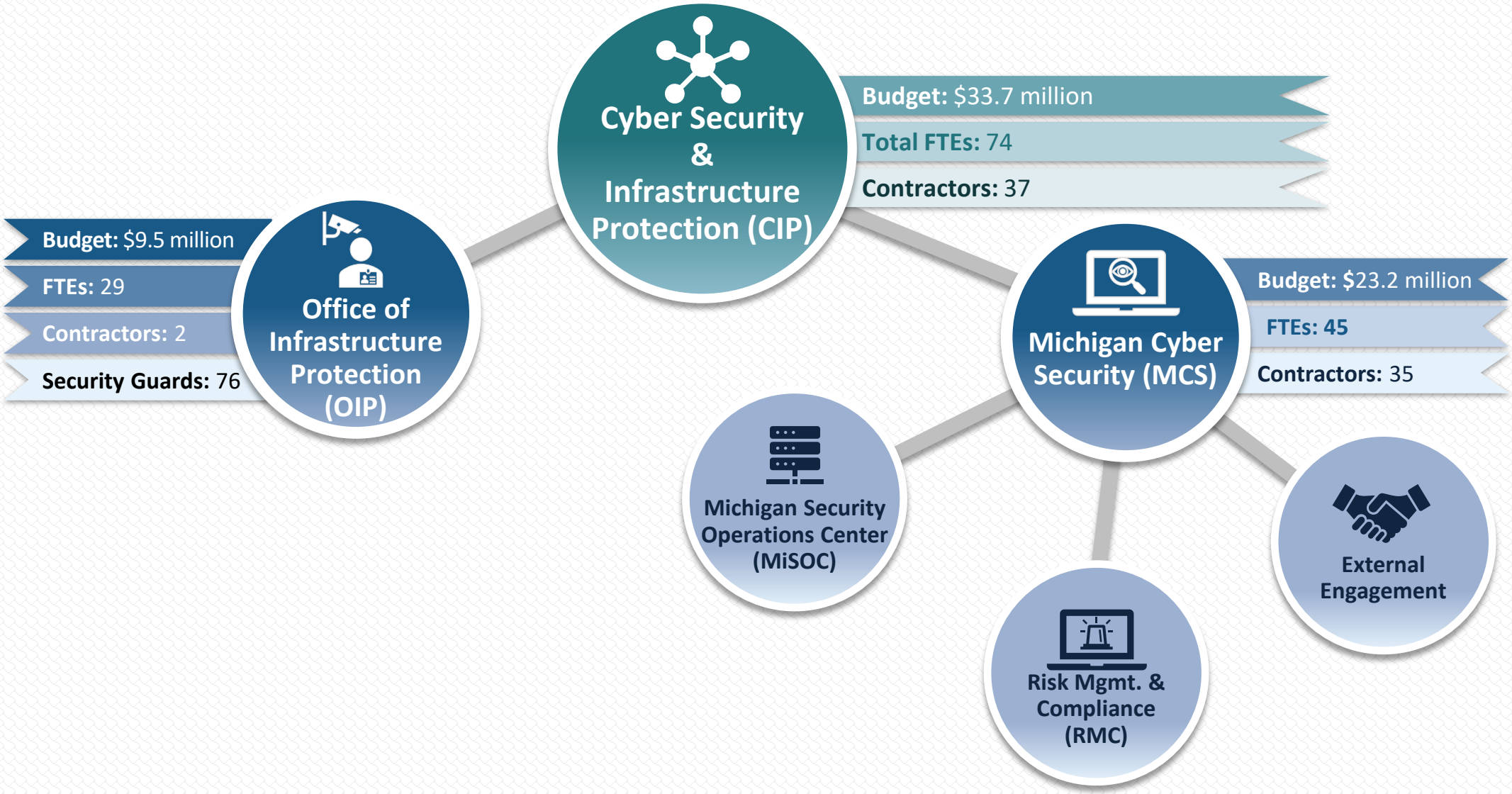
- Establish SecureMI programs.
- Continue to grow the Cyber Partnership Readiness Assessments.
- Enhanced IRT events.
- Refine Standard Operating Procedures to be used during cyber events.

2022+

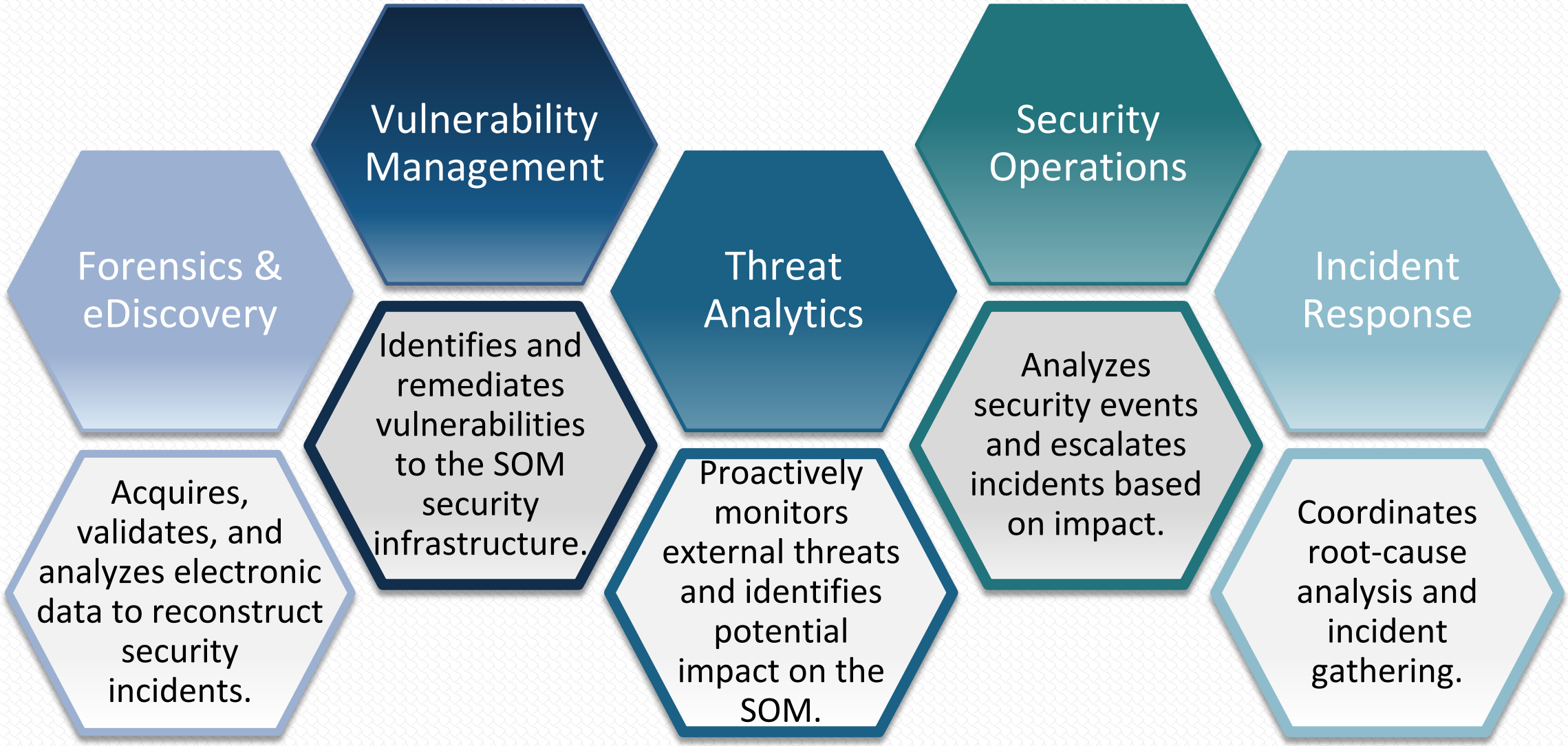
- Continue to explore projects that provide preventative protection to threats in the cyber ecology.
- Track and manage cyber threats as they happen.

- Survey Question

Cybersecurity and Infrastructure Protection



MCS – MiSOC Functions



MCS – Risk Management and Compliance Functions

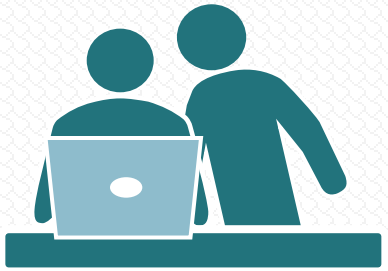
External Engagements

Cyber Partners Collaboration

- Quarterly meetings
- **Partnerships:** Local Governments
- **Actions:** Develops best practices in security budget, workforce, & training.

CSO Kitchen Cabinet

- Monthly meetings
- **Partnerships:** Regional businesses
- **Actions:** Develop cybersecurity and incident response strategies.



Michigan Health Care Cybersecurity (MIHCC)

- Monthly meetings
- **Partnerships:** Health care industry professionals
- **Actions:** Develop actionable recommendations for healthcare-specific security threats and challenges.

North American Int'l Cyber Summit

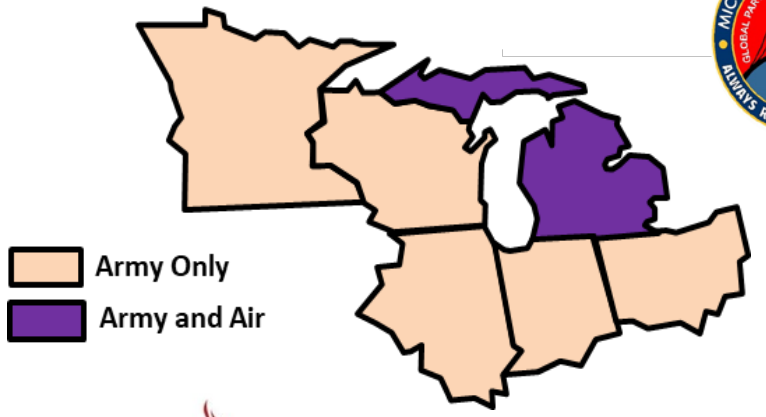
- Annual summit
- **Partnerships:** Regional, national, and international
- **Actions:** Provide a forum for leaders, professionals, and others to share cybersecurity knowledge and best practices.

MSP Highlights

- **Michigan Cyber Command Center (MC3)**
  - MC3 is the resource for cybersecurity and cybercrime awareness for critical infrastructure; federal, state, and local government entities; other public and private sectors; and citizens of the State of Michigan
- **Computer Crimes Unit (CCU)**
  - CCU is the statewide leader in responding to and investigating technology digital crimes and in providing forensic data recovery assistance
- **Internet Crimes Against Children Task Force (ICAC)**
  - In partnership with the CCU, the ICAC is a collection of state, local, and federal partners concentrating on child sexually abusive material trafficking as well as child sex exploitation investigations.

DMVA – National Guard Highlights

- **Army and Air Force Cyber Protection Teams**
  - Responsible to defend military networks
    - Identify, defend and counter cyber threats
    - Train, advise, and assist state or local government
    - Members engaged around the US for past 3 years
  - Expanding support to include state critical infra-structure inspections, vulnerability assessments, remediation
  - Partners
    - DoD, USAF, USA, USCC, DHS
    - Sister States/Nations
      - Canada, Latvia, Estonia, Lithuania
    - Industry, citizen Soldiers/Airmen
    - Academia, Cyber Patriot



JPMorgan Chase & Co.

FireEye

DOW

NUCOR

VDA LABS

FHLBank INDIANAPOLIS

GD

- Technical Expertise
- Business Acumen
- Industry Leadership Skills

- Military Training & Expertise
- Military Leadership
- Dedication, Esprit de Corps
- Patriotism

- Well-rounded and Dynamic
- Technically Savvy
- Seasoned Longevity

National Security Agency – United States of America

Wendy's

leidos

Rehmann

amazon

- Survey Question

Importance of DTMB's Continued Cyber Investment

Continued Investment Needs:

- Reduce vulnerabilities by scanning and patching software and hardware.
- Ensure custom applications and commercial systems are secure.
- Invest in security tools to detect threats and defend the State of Michigan network.
- Train DTMB resources in security and recruit security talent.
- Deploy tools to discover sensitive data and address vulnerabilities.
- Implement tools to better manage access to systems and data.

Questions?


THANK YOU